Biotic Prediction

Building the Computational Technology Infrastructure
for Public Health and Environmental Forecasting

Risk Management Plan

BP-RMP-1.0

Task Agreement: GSFC-CT-1

April 8, 2002

Contents

1 Overview

1.1 Introduction

This project will develop the high-performance, computational technology infrastructure needed to analyze the past, present, and future geospatial distributions of living components of Earth environments. This involves moving a suite of key predictive, geostatistical biological models into a scalable, cost-effective cluster computing framework; collecting and integrating diverse Earth observational datasets for input into these models; and deploying this functionality as a Web-based service. The resulting infrastructure will be used in the ecological analysis and prediction of exotic species invasions. This new capability will be deployed at the USGS Midcontinent Ecological Science Center and extended to other scientific communities through the USGS National Biological Information Infrastructure program.

1.2 Referenced Documents

Table 1. Referenced Documents

Document Title	**Version**	**Date**
Software Engineering / Development Plan	1.0	2002-04-08
Risk Management Plan	1.0	2002-04-08

1.3 Document Overview

This document, the *Risk Management Plan*, describes our plan for managing risk throughout the lifecycle of the project.

Section 2 describes our approach toward identifying and managing risk.

Section 3 has a list of risks we have identified, our assessments, and mitigation plans for them.

Appendix A has a glossary of some terms and acronyms used in this document.

2 Approach

Our overall approach for managing risk throughout the project involves the following steps: Identify, Assess, Analyze, Monitor, Mitigate.

2.1 Identify Risks

Throughout the project we will consider risks to the successful completion of the project. We will document those risks in the Risk Management Plan.

We will continually consider the project in light of risk and any new risks that come up will be added to the RMP

2.2 Assess Risks

Each risk will be openly discussed and analyzed. We will assess and document the probability of the risk occurring and the severity of the effect on the project if the risk did occur. We will use the following ratings for this assessment:

Probability:

High	The risk is more likely to occur.	$\gg 50\%$
Medium	The risk is about as likely to occur as not to occur.	$\approx 50\%$
Low	The risk is more likely not to occur.	$\ll 50\%$

Severity:

High	This risk, unmitigated, would result in a complete failure for the project.
Medium	This risk would have a major impact on the project's schedule, cost, or performance.
Low	This risk would have a minor impact on the project.

2.3 Analyze Risks

Based on the ratings given to each risk, they will be analyzed to determine what action the project will take. That action could include immediate programatic changes to ensure that the risk does not occur, development of mitigation plans that could be implemented in the event of the occurence of the risk, or some other action as appropriate.

2.4 Monitor Risks

Every effort will be made to ensure that the risks do not occur, and if they do occur, that we notice the occurence of the risk as soon as possible. Early notice can help us limit any possible negative effects of the risk on the project. If progression of the project changes the assessment of the probability or severity of a risk, the risk will be analyzed and the RMP will be updated.

2.5 Mitigate Risk

In the event that a risk does occur, the issue will be analyzed in light of the mitigation plans and action will be taken as appropriate.

3 Risks

3.1 Programmatic Risks

Personnel Availability		
Risk ID: P-1	**Probability:** Medium	**Severity:** Medium
DESCRIPTION: We have a number of individuals already identified to participate in this project. We are also planning on hiring some additional help. The individuals working on the project could become unavailable at some point in the future. We could also have difficulty finding the specific skills we need within our budget.		
ANALYSIS: We have a range of expertise available across multiple people. Much of the staff of the project are GSFC civil servants that yields some stability as well.		
PLAN: We have potential backup individuals that will work together to share knowledge so that no one person is critical to the success of the project. We also intend to thoroughly document work as it proceeds, minimizing the time to bring a new person up to speed if that does become necessary.		

Computer Security		
Risk ID: P-2	**Probability:** Low	**Severity:** Medium
DESCRIPTION: An unauthorized individual could break into our development machines.		
ANALYSIS: They could destroy programs or data in a noticable way, or worse, maliciously alter data such that we produce the wrong answers.		
PLAN: We will contract with the LTPCF to administer the primary development machine. All security measures recommended by the LTP Security plan will be put in place. The SA's will monitor security recommendations and patch any software as security patches become available. Additionally, logins to the host will be restricted to SSH. Non-GSFC developers will make deliveries of code and data through a one-way anonymous ftp drop box.		

Schedule Concerns		
Risk ID: P-3	**Probability:** Low	**Severity:** Medium

DESCRIPTION:

The schedule and milestones are codified into the contract and are not flexible.

ANALYSIS:

Because the funding for this project is dependent on producing specific products and meeting specific performance goals, the schedule is critical. Careful thought and negotiation before project initiation resulted in challenging but achiveable goals.

PLAN:

The PM will manage the project with the schedule and focus managment actions toward meeting the scheduled milestones. Regular meetings of key project personnel, at least bi-weekly, and milestone charts provide overall visibility to the PM.

Customer Buy-In		
Risk ID: P-4	**Probability:** Medium	**Severity:** Medium

DESCRIPTION:

We intend to produce this software to fulfill the needs of a scientific and application community. “Buy-in” represents the extent to which the software is acceptable to the customers and becomes used by them.

ANALYSIS:

Scientific communities are often slow to adopt new research methodologies. Using our software may involve an unpalatable paradigm shift in their research methodologies. We have, however, experience with many agencies and scientists open to new ways to solve problems and new ways of automating manual tasks.

PLAN:

We will work closely with the customer scientific community throughout the project, making them part of the requirements definition and staying responsive to their needs as we develop the software. We will have annual workshops to work directly with potential customers and ensure that the software is acceptable and useful for the community.

3.2 Technical Risks

Software Performance		
Risk ID: T-1	**Probability:** Low	**Severity:** Medium
DESCRIPTION: The software must meet specific performance goals for certain milestones.		
ANALYSIS: We have analyzed the underlying algorithms and believe performance improvement is possible. As we baseline the code, we will be working with the CT project to define specific performance goals.		
PLAN: We will work with the CT project to define performance goals that are realistic and achievable.		

Application Security		
Risk ID: T-2	**Probability:** Low	**Severity:** Medium
DESCRIPTION: The software product will include a WWW accessible front-end. This has the potential for network security issues.		
ANALYSIS: We intend to produce a software application that will be delivered to customers outside of this project and outside of NASA. The reputation of NASA, this project, and the individuals involved depends on producing a secure product.		
PLAN: We will make security a requirement for the system. We will analyze aspects of the software for security throughout the development life-cycle. We will use security expertise of our staff to the fullest.		

A Glossary

BP Biotic Prediction project

RMP Risk Management Plan

SEP Software Engineering / Development Plan

TBD To Be Determined or To Be Developed